

# **Laporan Ujian Akhir Semester Programming for Security Professional**



**UBAYA**  
UNIVERSITAS SURABAYA

F-22 Raptor:

160422018    Gabriel Narendra D.

160422073    Christopher

160423027    Merilee Alberta F. C.

# Executive Summary

This testing found several security issues in 3 OWASP Top 10, and the most critical part is in A07 : Identification and Authentication Failures, which has 4 Major failures. These errors were clearly identified easily and documented so this website can improve its flaws.

## Scope

Target : <https://psp.pengalilla.com>

Environment : Testing

Testing Type :

Tool Used : Burp Suite, nmap

*Authenticated User Access Provided (3 Hak Akses : User, Staff, Admin)*

## Methodology

Summary of Findings by OWASP Top 10

OWASP Category	Number of Findings
A01 – Broken Access Control	0
A02 – Cryptographic Failures	0
A03 – Injection	0
A04 – Insecure Design	2
A05 – Security Misconfiguration	0
A06 – Vulnerable and Outdated Components	0
A07 – Identification and Authentication Failures	4
A08 – Software and Data Integrity Failures	0
A09 – Security Logging and Monitoring Failures	2

A10 – Server-Side Request Forgery (SSRF)	0
--	---

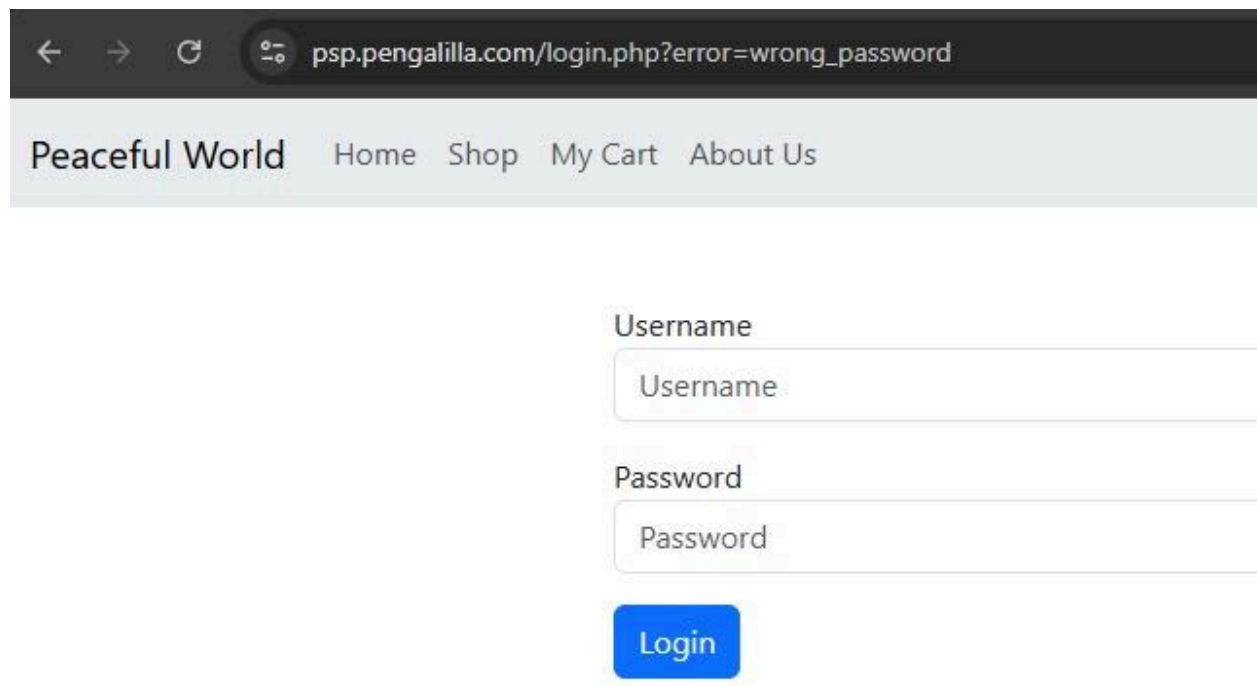
# Findings and Proof of Concept

## A04: Insecure Design

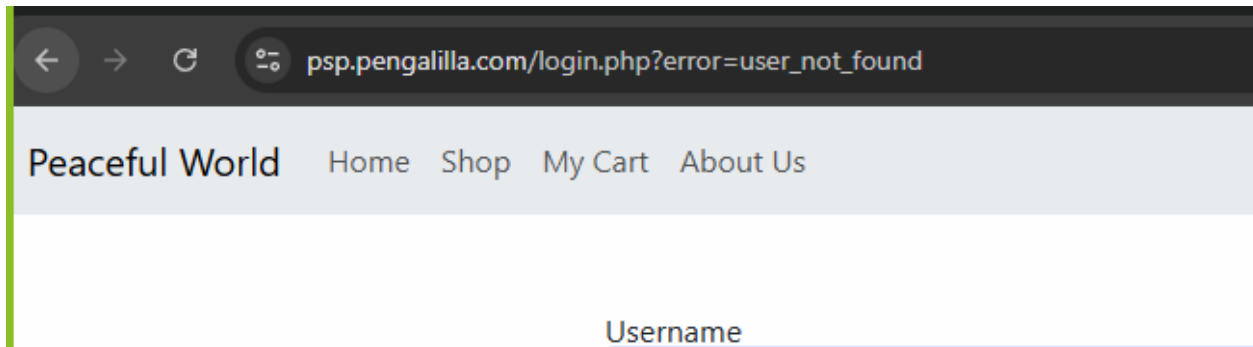
Description : No Login Attempt Limiter and Displaying Specific Error Message in Login

Result : Attacker know if username is correct or not, then brute force password

Screenshot :



The screenshot shows a web browser window with the address bar displaying `psp.pengalilla.com/login.php?error=wrong_password`. The page has a navigation bar with the text "Peaceful World" and links for "Home", "Shop", "My Cart", and "About Us". Below the navigation bar, there is a login form with two input fields: "Username" and "Password". The "Username" field contains the text "Username" and the "Password" field contains the text "Password". A blue "Login" button is positioned below the password field.



CVSS v3.0 Base Score :5.4

Vector String : CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

## **A07: Weak Password Authentication**

Description : No Complexity Enforcement, single char password is acceptable to system

Result : Very Quick Bruteforce

Screenshot :

CVSS v3.0 Base Score :7.1

Vector String : CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N

## **A07: No Multi-Factor Authentication**

Description :Does not implement Multi-Factor Authentication (MFA) on any login functionality

Result : Easy to Bruteforce, Not really secure as well

CVSS v3.0 Base Score :7.1

Vector String : CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N

## **A07: No Login Attempt Limiter**

Description: Does not implement any rate limiting

Result : The system provided consistent responses to failed logins, aiding automated attack tools. Brute-forceable

CVSS v3.0 Base Score : 6.5

Vector String : CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

## **A07: No Password Reset System**

Description: User can't reset their own password, purely based on memory

Result : User (any) can lose their account easily with no way of retrieving it

CVSS v3.0 Base Score : 5.3

Vector String : CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N



## A09: No Error Logging

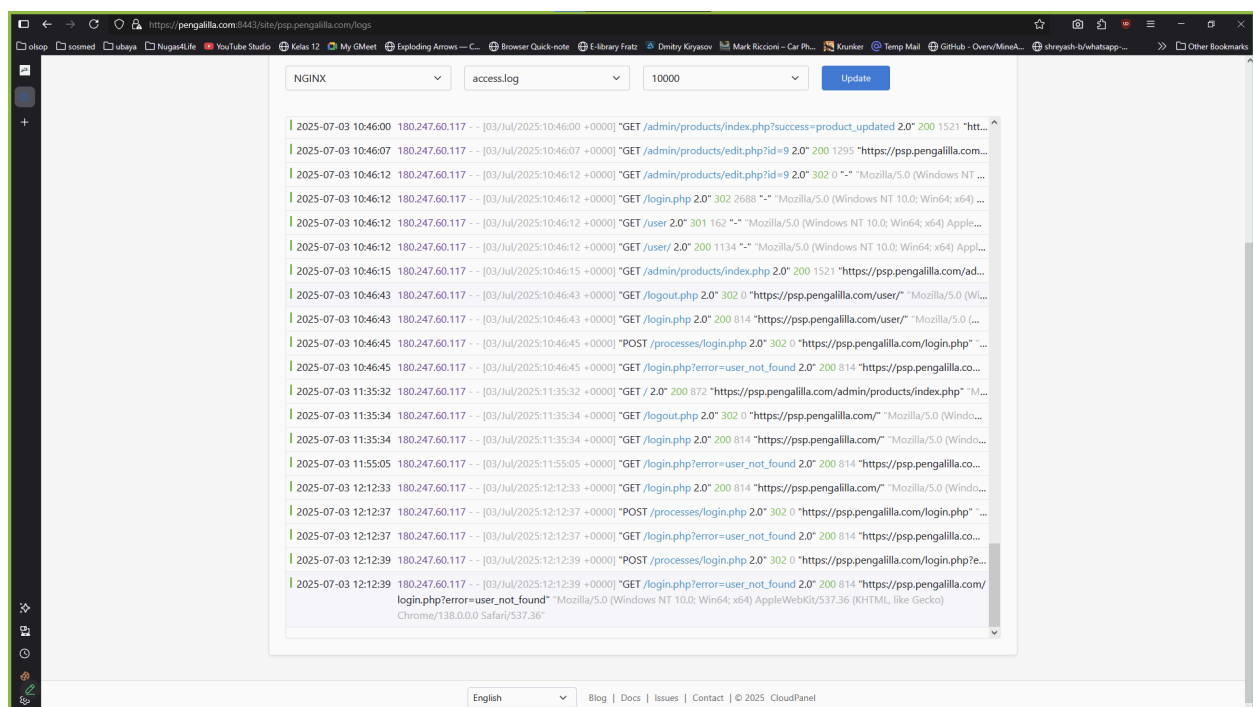
Description: Logging was implemented, but no ERROR or alerts were set

Result : Hard to trace any attacks

CVSS v3.0 Base Score : 4.2

Vector String : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Screenshot :



## **A09: No Security Information and Event Management**

Description: No SIEM Application connected to this web

Result : No Evidence or Alerts resulted

CVSS v3.0 Base Score : 5.5

Vector String : CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N